Identifying Program Risks

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

11 December 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **11 DEC 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE
Identifying Program Risks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

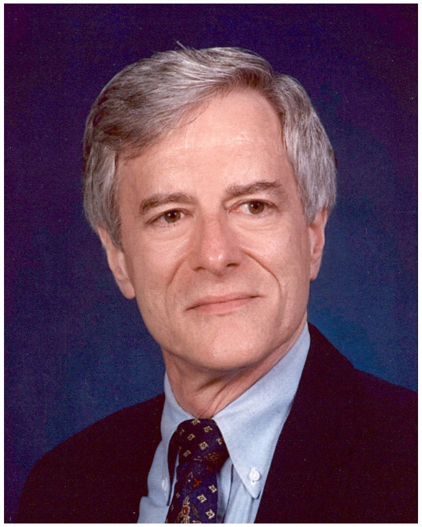
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**24**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Ray C. Williams



rcw@sei.cmu.edu

Ray Williams is a senior member of the technical staff at the SEI in the Acquisition Support Program (ASP). He was a member of the SEI Risk program from 1991 until the program was terminated in 1998 and was involved in the design and development of all its products. Since then he has served as steward of the Risk program’s legacy materials, primarily as lead instructor and course maintainer for the SEI’s Continuous Risk Management course. He has participated in and led many Software Risk Evaluations (SREs), and he co-developed and instructed the *Risk Management for Software Intensive Projects* masters-level course in CMU’s School of Computer Science. He has taught the *Introduction to CMMI* course twenty times for the SEI as a certified instructor. He has served for over six years as the VP of Administration for the PMI’s Risk Management Specific Interest Group (PMI RiskSIG).

Before coming to the SEI in 1991, Ray was an instrumentation design engineer for naval nuclear plants, a process engineer in the steel industry, and a software project manager in the construction industry.

Polling Questions

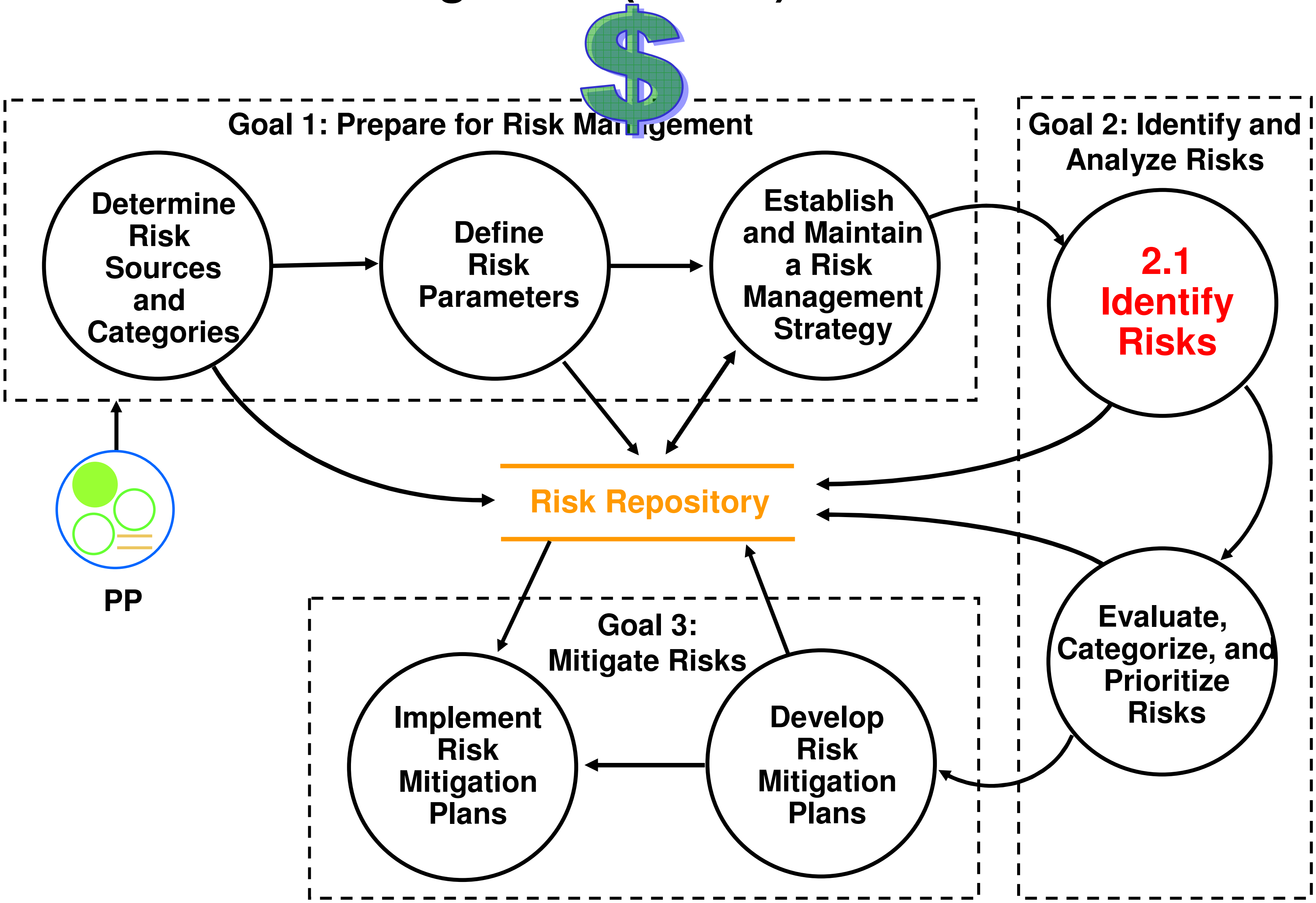
Polling Question 1: Give me a sense of how many of you are coming to this webinar from the perspective of the CMMI Risk Management Process Area:

- ○ I have completed an official Introduction to CMMI course.
- ○ I'm involved in doing risk management according to CMMI, but I haven't taken Introduction to CMMI.
- ○ I'm here because I'm interested in risk management and identifying risks, but not in CMMI.
- ○ None of the above/other.

Polling Question 2: I'd like to know whether you have risk management processes in place in your program or organization, and -- if so -- how "mature" you consider it to be:

- ○ We have had risk management in for some time -- it's well established and pretty mature.
- ○ We have risk management in place, but it's fairly new and not too well established.
- ○ We don't have risk management processes in place yet.

CMMI Risk Management (RSKM) Process Area


Goal 1: Prepare for Risk Management
Determine Risk Sources and Categories
Define Risk Parameters
Establish and Maintain a Risk Management Strategy
Goal 2: Identify and Analyze Risks
2.1 Identify Risks
Evaluate, Categorize, and Prioritize Risks
Risk Repository
PP
Goal 3: Mitigate Risks
Implement Risk Mitigation Plans
Develop Risk Mitigation Plans

Programs Often Don’t Document Real Risks

- Independent Technical Assessments (ITAs) and SCAMPI appraisals probe interviewees for top risks to the program.
- The “top risks” named by the interviewees often can’t be found in the programs risk repository.
- A risk repository that is visible to all is usually more *political* than *useful*.
- There is often no real, repeatable process in a program for identifying risks.

Developing Good Risk Identification Techniques Took Time

- Interviews and workshops with DOD program managers in the early 1990s pin-pointed risk identification as the biggest need.
- This became the first focus of the SEI risk program.
- 40 field tests were conducted with a broad range of software developers before coming up with a good interviewing technique for risk identification (the “Taxonomy-Based Risk Identification” method).
- Several more years passed before the Condition-Consequence risk statement form and the “Threshold of Success” were incorporated into the identification approach.

Threshold of Success (ToS)

- What is it?
  - The <u>minimum set of conditions</u> that MUST be met for your project members to consider the project a marginal "success"
- What does it have to do with risk statements?
  - Identified risk are evaluated against the conditions itemized in the program's ToS
  - Mapping risks to ToS conditions assures that appropriate attention is being paid to the risks with the biggest impact on the project's view of success
- When do I need one?
  - Any time you want to identify risks or categorize, evaluate, and prioritize a list of risks
  - Reevaluated when a major event takes places that has a direct impact on the project

How to Build a ToS

Define a **minimum set of conditions** the MUST be met for your project members to consider it a “Success”

Make sure these goals are **specific**, **measurable** and **set for a certain time in the future** (typically the end of the project) and that they are attainable and realistic

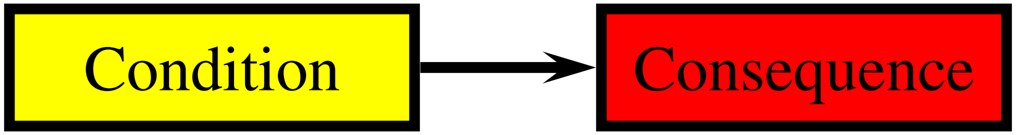
Guidelines

- Put yourself at the end of the project
- Build yourself a **picture of failure**
  - List those things it would take for your project to fail
  - Example: We did not meet “must have” requirements, We didn’t deliver on schedule etc’
- Convert those into Threshold of Success statements (we MUST do X or have shown that our product has met at least Y to reach our ToS)
- Stay within one slide limit with 4-5 items on it

Threshold of Success (ToS) — An Example

- Approval to continue the project at Key Decision Point 4 (KDP4) in late fall, 1999.
- Support from {Gov't Agency} management to maintain the 2001 budget at not less than $7M.
- People in the field are "begging" for {product} deployment (because they see that it will make their tasks so much easier), and
- A single point of entry for all logistic data (i.e., resolution of all issues with other responsibility areas within the {Gov't Agency} of where data comes from, what is the most reliable source of information, who will enter it, etc.)

The Condition-Consequence Risk Statement

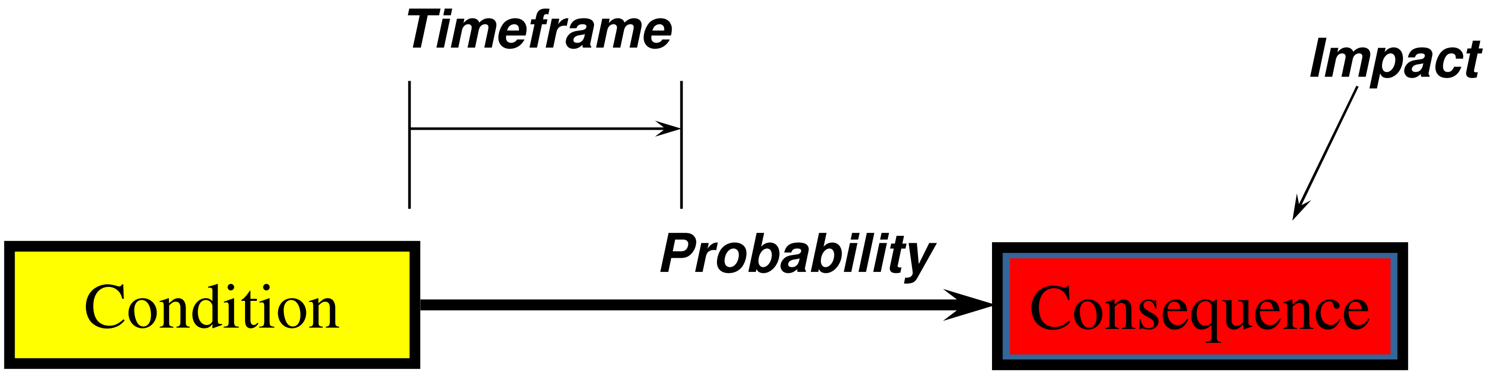


Condition

Consequence

The requirements for passing Milestone B have not yet been defined ; the current schedule and cost estimates may be inadequate.

The Condition-Consequence Form Supports Analysis

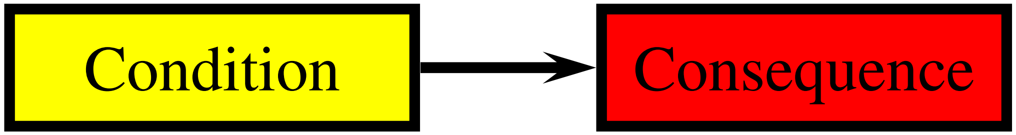


The requirements for passing Milestone B have not yet been defined ; the current schedule and cost estimates may be inadequate.

The Risk Statement

A “standard” format for risk statements provides:

- clarity
- consistency
- a basis for future risk processing



A good Risk Statement is

- fact-based
- actionable
- brief

A Simple Risk Identification Interview

Risk Statements from Interviews$_1$

- Lack of executive sponsorship (maybe because of change in the Administration); time delays, frustrations, credibility, and morale, and [a department co-sponsoring the project] may pull out of [the project].
- The majority of software-to-software interfaces are not defined & controlled; incomplete interfaces results in no benefits from [the project].
- There has been inadequate schedule discipline (milestones, slippage, monitor progress, good project management) on this project; with no intervention the project will continue to slip & slide.

Risk Statements from Interviews$_2$

- Unstable resources; leads to inability to plan.
- [The project] doesn't have a formal priority for resources; project slippage and waste of resources.
- "Shared Vision", but lack of agreement above & between agencies in means to reach objective; marginal utility of product and waste of resources.

Risk Statements in the "If-Then" Form

- It's too easy to start thinking up worries about the far future not based on anything going wrong today ("If our code gets written badly, then our product might not be accepted by customers")
- It's too easy for higher management to reject the underlying issue out of hand.
- People often masquerade their own desires for how the program should be managed as a "risk statement"; for example, "*If we're not able to hire enough programmers to do the development work by July, then we could deliver the product late*."

For Further Reading — SEI Publications on Risk Identification

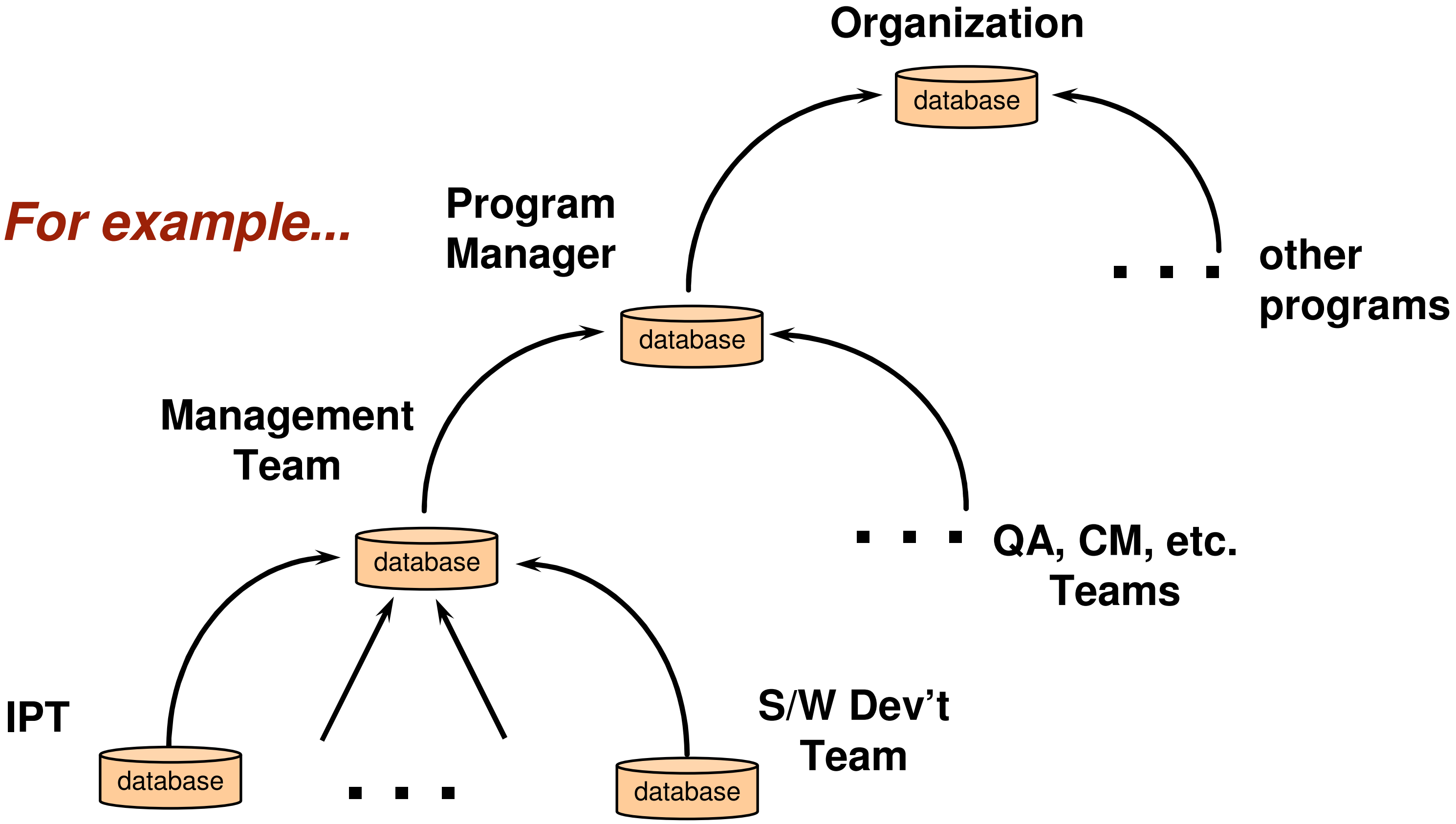
- CMU/SEI-93-TR-6, “Taxonomy-Based Risk Identification,” M.J. Carr et al
- CMU/SEI-94-TR-014, “A Construct for Describing Software Development Risks,” D. Gluch
- *Continuous Risk Management Guidebook*, August 1996, A.J. Dorofee et al (available only online at http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html)
- CMU/SEI-99-TR-029, “SRE Method Description (Version 2.0) & SRE Team Members Notebook (Version 2.0), R.C. Williams et al
- CD-ROM for CMU/SEI-99-TR-029, “Interviewing Process” (available free of charge from SEI Customer Relations – just call!)
- CMU/SEI-??-TN-???, “Mini Software Risk Evaluations: Going Light Evaluating Risks in Software Intensive Projects,” R.C. Williams and G. Taran

Setting the Stage for Good Risk Identification

- It appears to be commonly believed that the only possible form of a risk repository is one that contains all the program risks and is accessible to all program members.
- Some believe CMMI and the SEI expect this.
- In practice, this is the surest way to leave all the most important risks undocumented.
- An undocumented risk can get lost to everyone -- far better to have risks documented privately than not to be documented at all.
- If program management expects openness from “worker bees” and middle management about the risks they see, program management must likewise be open about their risks.

A Risk Repository can be Distributed and Locally Private

For example...



Summary

- A work team identifying risks needs to agree on an end-point against which to identify and analyze the risks.
- There needs to be a standard way of capturing (documenting) a risk.
- Facilitators need practice to become comfortable writing risks in front of a group.
- There are many ways for program management to support good risk identification:
    - Encourage documentation of risks privately at the working team level
    - Integrate risk identification and management into normal project management
    - Accept any risk identified into the repository – don’t “vet them out”
    - Acknowledge that the program’s decision-makers are the real “risk managers,” and have the decision-makers step up to the job

Related SEI Courses

There are public offerings of the SEI's *Continuous Risk Management* (CRM) course in 2009 on the following dates

- ☞ March 3-4 (Pittsburgh)
- ☞ June 23-24 (Pittsburgh)
- ☞ October 21-22 (DC)

There are public offerings of the SEI's *Systems Acquisition Survival Skills* (SASS) course -- which includes heavy emphasis on risk management -- on the following dates

- ☞ April 15-17 (Pittsburgh)
- ☞ July 21-23 (Pittsburgh)
- ☞ November 18-20 (DC)

MSCE Risk Management Offerings

The Mission Success in Complex Environments (MSCE) initiative at the SEI has the following offerings available as individual client engagements:

- ☞ Risk Management Tutorial – A one-half day tutorial that provides an overview of practical, success-driven risk management concepts.
- ☞ Risk Management Workshop – A one-day workshop that presents a practical risk management framework and teaches how to assess a risk management capability against the framework.
- ☞ Risk Management Clinic – A two-day workshop focused on improving an organization’s risk capability to achieve practical, effective management of risks to program objectives.

Contact customer-relations@sei.cmu.edu for more information

A Related Podcast

"Culture, Psychology, and Motivation: Getting Program Decision-Makers to Use and be Part of Risk Management Processes“

A panel session presentation recorded live at the 2007 INCOSE International Symposium

http://www.sei.cmu.edu/programs/acquisition-support/rw_w_bumpers.mov

Software Engineering Institute | Carnegie Mellon